	COUNTY OF SAN BERNARDINO STANDARD PRACTICE	NO.: 2-312	ISSUE: 1 Page 1 of 3 EFFECTIVE: 2/11/2005
		BY: Kathie Pelletier, Program Manager	
DEPARTMENT: PUBLIC HEALTH		APPROVED:	
SUBJECT: Information Security Health Insurance Portability and Accountability Act (HIPAA) **Administrative, Physical and Technical Safeguards**		James A. Felten, Public Health Director	

I. POLICY:

Department of Public Health (DPH) Programs affected by the Health Insurance Portability and Accountability Act (HIPAA) shall implement appropriate administrative, physical and technical safeguards to reasonably protect the privacy of Protected Health Information (PHI).

II. PURPOSE:

The purpose of this Standard Practice is to establish the criteria for safeguarding PHI and to minimize the risk of unauthorized access, use or disclosure. It specifies actions that should be implemented to ensure the privacy of an individual's PHI.

III. PROCEDURES:

A. Administrative Safeguards

1. Determine and document the workforce members who require access or use of PHI to do their jobs.
2. Ensure only those workforce members have access to PHI.
3. Limit PHI access to only the amount necessary for workforce members to do their jobs.
4. Ensure workforce members read DPH HIPAA Standard Practices.
5. Ensure workforce members receive on-going HIPAA training as may be deemed necessary by either the Department or Program and document participation in training.

B. Physical Safeguards

1. **Oral safeguards**:
   a. Protect the privacy of verbal discussions involving the use or disclosure of PHI.
   b. Modify discussions involving PHI based on risk level of the immediate surroundings.

   Risk levels are:
   - Low Risk A low risk location is where there is absolutely no client or employee traffic. Examples of low risk level locations are interview rooms, enclosed offices or conference rooms.
   - Medium Risk A medium risk location is where there is little client or employee traffic. Examples include employee only areas and individual cubicles.
   - High Risk A high-risk location is one in which there is frequently client and employee traffic. Examples include public areas, reception areas and shared cubicles housing multiple staff where clients may be present.

2. **Visual Safeguards**

a. **Computer Data**

- Use polarized screens or overlay devices to ensure screens are not visible
- Place computers out of the visual range of unauthorized persons
- Clear PHI from the screen when not being used
- Implement an "Automatic Computer Screen Lock" when computers are not in use for a specified period of time (See attachment A)

b. **Documents in Use**

- Store documents in lockable desks or file rooms
- Ensure open area storage systems are locked
- Obtain lockable storage if none are available
- Turn documents upside down when an employee leaves his or her desk

d. **Record Retention Safeguards**

Programs shall make certain storage rooms containing PHI awaiting disposal are locked after business hours or when authorized staff are not present.

c. **Disposal or Destruction**

- Desk-site containers containing PHI to be disposed of shall be clearly labeled "confidential" and shredded daily
- Centralized waste/shred bins shall be clearly labeled "confidential", sealed and placed in a lockable storage room
- Procedures shall be implemented to minimize risk if lockable storage areas or bins are not available
- Shred paper documents in accordance with retention time requirements

C. Technical Safeguards

Examples of technological safeguards may include:

1. Computer pass codes
2. Automatic timing out of computer monitors
3. Firewalls
4. Encrypting PHI
5. Patches and Hot Fixes
6. Antivirus Protection
7. Software and/or hardware programs designed to prevent unauthorized access

D. Miscellaneous Safeguards

1. **Incidental Disclosures**

   Implement any additional administrative, physical and technical safeguards as appropriate to reasonably limit incidental disclosures.

2. **De-Identifying Data**

   De-identified data neither identifies nor provides a reasonable basis to identify the individual(s) to whom the information refers. Consequently, there are no restrictions on the use and disclosure of de-identified health information. When feasible, de-identify health information by removing all unique identifiers.

3. **Faxing PHI**

   - Use a coversheet that labels the transmission as confidential
   - Confirm that the fax number used is correct prior to submission
   - Place the fax machine in a secure location
   - Telephone recipient prior to faxing to alert them that the fax is being sent

4. **Answering Machines**

   - To confirm an appointment, leave only the information necessary to confirm the appointment or request a callback.
   - Avoid referencing what the appointment is for and do not state the physician's specialty (e.g. Gynecologist, Oncologist, etc.)

5. **Patient Sign-In Sheets**

   Ensure sign-in sheets are not requesting medical information that is not necessary for the purpose of signing in.

6. **Announcing Patient Names**

   - Limit the information disclosed over the system and/or
   - Refer patients to a reception desk where they may receive further instructions in a more confidential manner

7. **Patient Charts**

   When patient names are displayed on the outside of patient charts:

   - Limit access to areas where patient charts are displayed
   - Ensure the area is supervised
   - Ensure non-employees are escorted when in the area
   - Place patient charts in such a way that the writing is not visible to passers by

8. **X-Ray Light Boards and White Boards**

   - Make sure white boards are not readily accessible or visible to the public
   - Implement any other safeguards that reasonably limit incidental disclosures

Questions? Call the HIPAA Hotline @ (909) 387-6205